

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-078235

(43)Date of publication of application : 14.03.2000

(51)Int.Cl.

H04L 29/08  
G09C 1/00  
H04L 12/66  
H04L 12/54  
H04L 12/58

(21)Application number : 10-241699

(71)Applicant : NIPPON TELEGR & TELEPH CORP  
<NTT>

(22)Date of filing : 27.08.1998

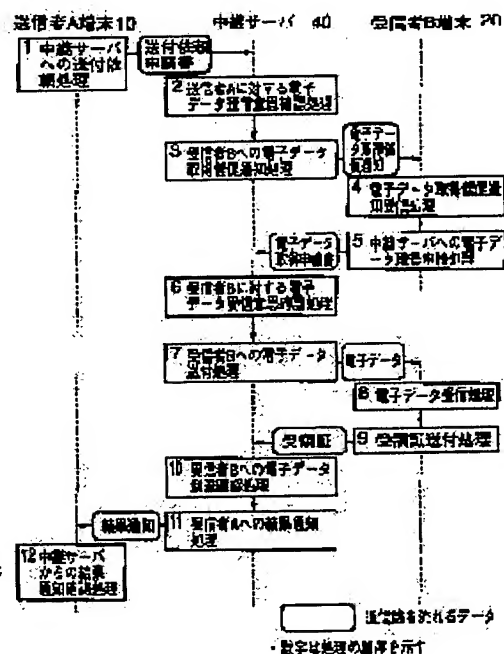
(72)Inventor : HASHIMOTO SHOICHI

## (54) ELECTRONIC DATA ARRIVAL WARRANTEE METHOD, ELECTRONIC DATA RELAY SYSTEM AND PROGRAM RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To certify the fact for a 3rd party that a sender A transmitted electronic data to a recipient B and that the latter had the intention of receiving the electronic data.

SOLUTION: A sender A transmits a transmission request, including electronic data and a name of a recipient B to a relay server 40, which stores the transmission request sheet and informs a recipient B of the storage of the electronic data addressed to the recipient B together with its identifier. The recipient B generates an acquisition application sheet and sends it to the server 40. The server 40 confirms that the acquisition application sheet is sent from the recipient B and a transmission destination of electronic data with the identifier matches the recipient B, stores the acquisition application sheet and transmits the electronic data designated by the identifier in the acquisition application sheet to the recipient B. The recipient B generates reception confirmation information, specifying the electronic data definitely and sends a receipt including the information and the identifier to the server 40, and the server 40 confirms that the reception confirmation information is identical to the electronic data designated by the identifier and stores the receipt.



## LEGAL STATUS

[Date of request for examination] 20.10.2000

[Date of sending the examiner's decision of rejection] 21.05.2002

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection] 2002-11286

[Date of requesting appeal against examiner's decision of rejection] 20.06.2002

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号 ✓  
特開2000-78235  
(P2000-78235A)

(43) 公開日 平成12年3月14日 (2000.3.14)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	キーワード (参考)
H 0 4 L 29/08		H 0 4 L 13/00	3 0 7 A
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00	6 4 0 B
	6 6 0		6 6 0 G
H 0 4 L 12/66		H 0 4 L 11/20	B
12/54			1 0 1 Z
審査請求 未請求 請求項の数 9 O L (全 9 頁) 最終頁に続く			

(21) 出願番号 特願平10-241699

(22) 出願日 平成10年8月27日 (1998.8.27)

(71) 出願人 000004226

日本電信電話株式会社

東京都千代田区大手町二丁目3番1号

(72) 発明者 橋本 正一

東京都新宿区西新宿三丁目19番2号 日本  
電信電話株式会社内

(74) 代理人 100066153

弁理士 草野 卓 (外1名)

## (54) 【発明の名称】 電子データ到達保証方法、電子データ中継システム及びプログラム記録媒体

## (57) 【要約】

【課題】 送信者Aが受信者Bへ電子データを送付した事実、Bが電子データを受信する意志があったことなどを第三者に対して証明可能とする。

【解決手段】 Aは電子データとBを含む送付依頼書の中継サーバ40に送り、中継サーバは送付依頼書を保管し、B宛の電子データを保管していることをその識別子と共にBへ通知する。Bは取得申請書を作り、サーバ40へ送り、サーバ40は取得申請書がBから送られたものを、その識別子の電子データの送付先がBと一致することを確認して、取得申請書を保管し、申請書の識別子で指定された電子データをBへ送る。Bは電子データを一意に特定可能な受領確認情報を作り、これと識別子を含む受領書をサーバ40へ送り、サーバ40は受領確認情報が識別子の電子データと同一のものであることを確認して、受領証を保管する。

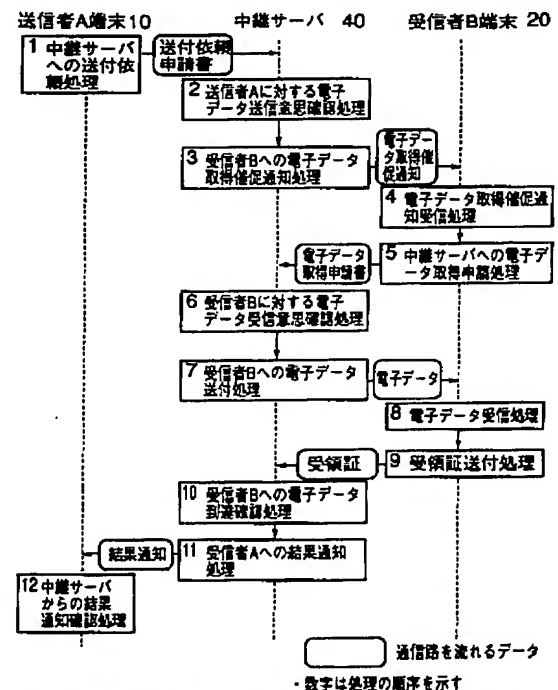


図 2 本発明における電子データ到達保証方法を実現するための処理の流れ

## 【特許請求の範囲】

【請求項 1】 コンピュータネットワークを介して送信者 A 端末が受信者 B 端末に電子データを送信する時、送信者 A 端末と受信者 B 端末との間で電子データの送付を仲介し、その仲介事実を保証するための電子データ通信手段、公開鍵証明証取得手段、電子署名検証手段、電子データ保管手段及び受領確認情報確認手段を有する中継サーバと、

中継サーバに対して受信者 B 端末への送付を依頼するための電子データ編集手段、電子署名生成手段、電子データ通信手段と、中継サーバからの依頼に対する結果を確認するための電子データ表示手段とを有する送信者 A 端末と、

中継サーバからの電子データの受理と引き換えに受理した証を中継サーバへ返すための電子データ編集手段、電子署名生成手段、電子データ通信手段及び、受領確認情報生成手段を有する受信者 B 端末と、  
公開鍵証明証を配送する手段を有する認証システムとからなる電子データ中継システム。

【請求項 2】 送信者端末において、電子データ編集手段を用いて送付対象電子データ及び送付先情報を含んだ送付依頼申請書を作成し、電子署名生成手段を用いて送付依頼申請書に対する送信者 A の電子署名を生成し、電子データ通信手段を用いて電子署名が付与された送付依頼申請書を中継サーバへ送付し、  
中継サーバにおいて、電子データ通信手段を用いて送信者端末が送付した送付依頼申請書を受理後、公開鍵証明証取得手段を用いて送信者 A の公開鍵証明証を認証システムから取得し、電子署名検証手段を用いてこの公開鍵証明証内に含まれる公開鍵により送付依頼申請書に付与された電子署名を検証し、送付依頼申請書内に送付対象電子データ及び送付先情報が存在することを確認した後に、電子データ保管手段を用いて送付依頼申請書を保管することにより、送信者 A が確かに送付依頼申請書に含まれる電子データを送付先情報として指定された受信者 B へ送付する意志があった事実を確認し、その証拠情報を保管することを特徴とする電子データ到達保証方法。

【請求項 3】 中継サーバにおいて、電子データ通信手段を用いて中継サーバが受信者 B 宛の電子データを保管していること及びこれを取得するための識別子を受信者 B 端末に通知し、  
受信者 B 端末において、電子データ通信手段を用いて中継サーバからのこの通知を受理した後、電子データ編集手段を用いて識別子に対応する電子データを取得するための電子データ取得申請書を作成し、電子署名生成手段を用いて電子データ取得申請書に対する受信者 B の電子署名を生成し、電子データ通信手段を用いて電子署名が付与された電子データ取得申請書を中継サーバへ送付し、  
中継サーバにおいて、電子データ通信手段を用いて受信

者 B 端末が送付した電子データ取得申請書を受理後、公開鍵証明証取得手段を用いて受信者 B の公開鍵証明証を認証システムから取得し、電子署名検証手段を用いてこの公開鍵証明証内に含まれる公開鍵により電子データ取得申請書に付与された電子署名を検証して、取得対象識別子に対応する電子データの送付先情報と電子データ取得申請書が一致していることを確認し、電子データ保管手段を用いて電子データ取得申請書を保管することにより、送信者 A 端末が送付した電子データを受信者 B が受理する意志があった事実を確認し、その証拠情報を保管することを特徴とする電子データ到達保証方法。

【請求項 4】 請求項 3 記載の方法において、  
中継サーバにおいて、上記電子データ取得申請書を保管後に、電子データ通信手段を用いて送信者 A 端末が送付を依頼した電子データを受信者 B 端末へ送付し、  
受信者 B 端末において、電子データ通信手段を用いて中継サーバが送付した電子データを受信し、受領確認情報生成手段を用いて受理した電子データを一意に特定可能な受領確認情報を生成し、データ編集手段を用いて少なくとも受領確認情報と電子データ取得申請書で指定した識別子を含む受領証を生成し、電子署名生成手段を用いて受領証に対する受信者 B の電子署名を生成し、電子データ通信手段を用いて電子署名が付与された受領証を中継サーバへ送付し、

中継サーバにおいて、電子データ通信手段を用いて受信者 B 端末が送付した受領証を受理後、公開鍵証明証取得手段を用いて受信者 B の公開鍵証明証を認証システムから取得し、電子署名検証手段を用いてこの公開鍵証明証内に含まれる公開鍵により受領証に付与された電子署名を検証して、受領証内に示された識別子に対応する電子データの送付先情報と受領証の送付者が一致していることを確認し、受領確認情報確認手段を用いて受領証内に含まれる受領確認情報が識別子に対応する電子データと同一の電子データを指し示すことを確認し、電子データ保管手段を用いて受領証を保管することにより、送信者 A 端末が送付した電子データを受信者 B 端末が確かに受理した事実を確認し、その証拠情報を保管することを特徴とする電子データ到達保証方法。

【請求項 5】 請求項 4 記載の方法において、  
中継サーバにおいて、上記受領証を保管後に、電子データ通信手段を用いて送付結果を送信者 A 端末へ送付し、  
送信者 A 端末において、電子データ通信手段を用いて中継サーバから結果通知を受理し、電子データ表示手段を用いて受信者 B 端末へ電子データが到達したことを確認することにより、送信者 A 端末が送付した電子データを受信者 B 端末が確かに受理した事実を、送信者 A が確認することを特徴とする電子データ到達保証方法。

【請求項 6】 送信者 A 端末より受信した送付対象電子データ及び送付先情報を含む送付依頼申請書に対する電子署名をその送信者 A の公開鍵により検証する処理と、

その検証に合格すると、上記送付依頼申請書を保管する処理と、  
 上記送付先情報である受信者B宛の電子データを保管していること及び、その電子データの識別子を受信者B端末へ送信する処理と、  
 を中継サーバのコンピュータに実行させるプログラムを記録した記録媒体。

【請求項7】 請求項6記載の記録媒体において、  
 受信者B端末より受信した電子データ取得申請書に対する電子署名を、受信者Bの公開鍵により検証する処理と、

その検証に合格すると、  
 上記電子データ取得申請書から取得した識別子と対応する電子データの送付先情報と、電子データ取得申請書の申請者が一致していることを確認する処理と、

その確認に合格すると、上記電子データ取得申請書を保管する処理と、

上記識別子と対応する上記保管した電子データを上記受信者B端末へ送信する処理と、

を上記コンピュータが実行するプログラムを上記プログラムが有することを特徴とする記録媒体。

【請求項8】 請求項7記載の記録媒体において、  
 受信者B端末より受信した受領証に対する電子署名を受信者Bの公開鍵により検証する処理と、

その検証に合格すると、受領証内に示された識別子に対応する電子データの送付先情報と、受領証の送付者が一致していることを確認する処理と、

受領証内に含まれる受領確認情報が、識別子に対応する保管中の電子データと同一の電子データを指し示すことを確認する処理と、

これらの確認に合格すると、受領証を保管する処理と、  
 を上記コンピュータが実行するプログラムを上記プログラムが有することを特徴とする記録媒体。

【請求項9】 請求項8記載の記録媒体において、  
 上記受領証を保管後に、送付結果を送信者A端末へ送付する処理を上記コンピュータが実行するプログラムを上記プログラムが有することを特徴とする記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 この発明は、コンピュータネットワーク上でEDI（電子データ交換）やEC（電子商取引）を実現するために必要となる電子データの送受信方式において、送付した電子データを確かに通信相手が受理したことを確認する方法及び、データの中継システム及びプログラム記録媒体に関するものである。

【0002】

【従来の技術】 コンピュータネットワークを介して電子データを送受信する場合に、なりすましや改竄（かいざん）などの脅威を防御し、受信者が電子データの送信元の本人性を確認する方式として、電子署名通信が一般に

用いられている。この電子署名通信を実現する暗号技術としては、公開鍵暗号方式であるRSAやESIGNなどが広く知られているところとなっており、送信者側における電子署名生成手段と、受信者側における電子署名検証手段を対で利用することにより電子署名通信が実現される。また公開鍵暗号方式を用いた電子署名通信において、署名付与者の本人性を確実に確認するための方法としては、認証システムと呼ばれる第三者機関が発行する公開鍵証明書により、その所有者が保証された公開鍵を用いて署名検証を行う方法が世の中で広く知られるところとなっている。

【0003】 さて、この電子署名通信が利用可能な状況において、送信者Aと受信者Bがコンピュータネットワークを介して電子データを送受信する場合に、送付した電子データが確かに受信者Bに受理されたことを送信者Aが確認可能となる一般的な方法としては、次の手法が考えられる。即ち図4に示すように、送信者A端末10における電子データ送付処理において、電子データ編集手段111で送信すべき電子データを編集し、この電子データに対し、電子署名生成手段112で電子署名を作成し、この署名を電子データに付け電子データ通信手段113により、受信者B端末20へ送信する。

【0004】 受信者B端末20における電子データ受信処理において、電子データ通信手段213により電子データを受信し、公開鍵証明書取得手段214により認証システム30から送信者Aの公開鍵証明書を受領し、その公開鍵により、電子データ署名検証手段215で、受信電子データの署名を検証し、その検証に合格すると、受信電子データを電子データ保管手段216に保管する。

【0005】 その後、受信者B端末20は受領証作成処理において、電子データ編集手段211により、電子データを受理したことを通知する受領証を作成し、その受領証に対する受信者Bの電子署名を電子署名生成手段212で生成し、その署名を受領証に付けて電子データ通信手段213により送信者A端末10へ送信する。最後に送信者A端末10における受領証確認処理において、電子データ通信手段113で受領証を受信し、公開鍵証明書取得手段114で認証システム30から受信者Bの公開鍵証明書を取得し、その公開鍵を用いて電子データ署名検証手段115で受領証に対する署名を検証し、その検証に合格すると、受信した受領証を電子データ保管手段116に保管する。

【0006】 ここで、送受信される電子データや受領証に対しては、データを送付する側で電子署名の付与を、受信する側で電子署名の検証を行い、改竄やなりすましが無いことを受信側において確認する。また受領証の構成内容は、送信者Aと受信者Bとの間であらかじめ任意に規定されたものが使用されている。

【0007】

【発明が解決しようとする課題】送信者A端末10が送付した電子データを確かに受信者B端末20が受理したことを、受信者B端末20が送付する受領証を用いて送信者A端末10が確認する場合、従来方法においては、送信者A端末10が送付した電子データと受信者B端末20が作成する受領証とが関連付けられていないため、当事者以外の第三者が、この受領証によって受信者B端末20による対象電子データの受理の事実を確認することができない。したがって、後日、受信者Bが悪意を持って故意に送信者A端末10から送付された電子データの受信事実を否認するなどの当事者間における紛争が生じた場合、紛争を解決するために第三者に対して提示可能な証拠情報がなく、電子データが受信者B端末20へ送付された事実を第三者に対して証明する手段がない。

【0008】また従来技術において受領証が送信者A端末10に送付されてこない場合には、送信者A端末10が送付した電子データを受信者B端末20が受理した事実はもちろん、送信者A端末10が受信者B端末20に対して電子データを送付した事実や、受信者B端末20が電子データを受理する意志があった事実を確認してこれを証明することができないという問題があった。

【0009】そこでこの発明では、送信者A端末が受信者B端末へ電子データを送付する過程において、送信者A端末が受信者B端末に対して電子データを送付した事実及び、受信者B端末が電子データを受理する意志があった事実及び、送信者A端末が送付した電子データを受信者B端末が確かに受理した事実を確認し、これらの事実を当事者以外の第三者に対して証明可能となる電子データ到達保証方法を提供し、またこの方法を実現する電子データ中継システムを構築すること、更にそのために各部で用いるプログラム記録媒体を提供することを目的とする。

【0010】

【課題を解決するための手段】コンピュータネットワークを介して送信者A端末が受信者B端末に電子データを送付する時、送信者A端末が送付した電子データを受信者B端末が確かに受理したことを確認し、この事実を当事者以外の第三者に対して証明可能とするために、この発明では、図1に示す装置構成に示すように電子データの送受信に中継サーバ40を介在させ、この中継サーバ40が送信者A端末10から受信者B端末20へ電子データの中継する過程において、(A)送信者Aが確かに電子データを受信者B端末20へ送付する意志があった事実及び、(B)送信者A端末が送付した電子データを受信者Bが受理する意志があった事実及び、(C)送信者A端末が送付した電子データを受信者B端末が確かに受理した事実を確認し、それぞれ確認に用いた電子情報を証拠情報として保管するところに特徴がある。以下では、送信者A端末10と受信者B端末20の間に介在した中継サーバ40において、(A)～(C)の事実を確

認しその証拠情報を保管する手段について、図2を用いて説明する。

【0011】(A)送信者Aが確かに電子データを受信者B端末へ送付する意志があった事実の確認及びその証拠情報の保管手段

1：中継サーバへの送付依頼処理

送信者A端末10は、送付対象である電子データと、その送付先情報とを最低限含んだ送付依頼申請書を作成し、これに自端末(送信者A端末)10が作成したことの証を含めて中継サーバ40へ送付する。

2：送信者Aに対する電子データ送信意志確認処理

中継サーバ40は、1の送付依頼申請書を受理し、これが確かに送信者A端末10から送付されてきたこと及び、送付対象電子データ及び送付先情報の存在を確認し、この送付依頼申請書を保管する。

【0012】以上により、中継サーバ40において、送信者Aが確かに送付依頼申請書に含まれる電子データを、送付先情報で示された受信者B端末へ送付する意志があった事実を確認し、その証拠情報の保管を実現する。

(B)送信者A端末が送付した電子データを受信者Bが受理する意志があった事実の確認及びその証拠情報の保管手段

3：受信者B端末への電子データ取得催促通知処理

中継サーバ40は、送信者A端末から受理した受信者B端末宛の電子データを保管していること及びこれを取得するための識別子を受信者B端末に対して通知し、これを取得することを促す。

4：電子データ取得催促通知受信処理

受信者B端末は、中継サーバ40からの3の通知を受理する。

5：中継サーバへの電子データ取得申請処理

受信者B端末20は、識別子に対応する電子データを取得するための電子データ取得申請書を作成し、これに自端末(受信者B端末)20が作成したことの証を含めて中継サーバ40へ送付する。

6：受信者Bに対する電子データ受信意志確認処理

中継サーバ40は、5の取得申請書を受理し、これが確かに受信者B端末20から送付されてきたこと及び、この取得申請書に示された識別子に対応する電子データの送付先情報が、取得申請書の送付者である受信者B端末と一致していることを確認し、この取得申請書を保管する。

【0013】以上により、中継サーバ40において、送信者A端末10が送付した電子データを受信者Bが受理する意志があった事実を確認し、その証拠情報の保管を実現する。

(C)送信者A端末が送付した電子データを受信者B端末が確かに受理した事実の確認及びその証拠情報の保管手段

## 7: 受信者B端末への電子データ送付処理

中継サーバ40は、受信者B端末20に対して電子データ取得申請書で指定された識別子に対応する電子データを送付する。

## 8: 電子データ受信処理

受信者B装置20は、7で送付された電子データを受理する。

## 9: 受領証送付処理

受信者B端末は、8で受理した電子データを一意に特定可能となる受領確認情報を生成し、少なくとも受領確認情報と取得申請書で指定した識別子を含む受領証を作成後、これに自端末(受信者B端末)20が作成したことの証を含めて中継サーバ40へ送付する。

## 10: 受信者B端末への電子データ到達確認処理

中継サーバ40は9で送付された受領証を受理し、これが確かに受信者B端末から送付されてきたこと及び、この受領証に含まれる識別子に対応する電子データの送付先情報が、受領証の送付者である受信者B端末20と一致していることを確認するとともに、受領証内に含まれる受領確認情報が、識別子に対応する電子データと同一の電子データを指し示すことを確認し、この受領証を保管する。

【0014】以上により、中継サーバ40において、送信者A端末10が送付した電子データを受信者B端末20が確かに受理した事実を確認し、その証拠情報の保管を実現する。そして、1~10の処理の後に、中継サーバ40における11送信者A端末10への結果通知処理において、中継サーバ40から受信者B端末20への電子データの送付結果を通知し、送信者A端末10における12中継サーバ40からの結果通知確認処理において、11で送付された結果通知を受理し、受信者B端末20への電子データの到達を確認することにより、送信者A端末10が送付した電子データを受信者B端末20が確かに受理した事実を、送信者A端末10が確認することが可能となる。

## 【0015】

【発明の実施の形態】この発明を実現するための具体的な実施例を図1、図3に示す。

## 1: 中継サーバへの送付依頼処理

送信者A端末10は、受信者B端末20への電子データの送付を中継サーバ40に依頼するため、電子データ編集手段111を用いて送付対象である電子データ及び送付先情報を最低限含んだ送付依頼申請書を作成し、電子署名生成手段112を用いてこの申請書に対する送信者Aの電子署名を生成し、電子データ通信手段113を用いて電子署名が付与された送付依頼申請書51を中継サーバ40へ送付する。

【0016】電子データ編集手段111は、コンピュータシステムが一般的に提供するエディタ機能やファイル読み込み機能を利用することにより、送付対象である電

子データ及び送付先情報を最低限含んだ送付依頼申請書を作成することが可能である。また、電子署名生成手段112は、既存のRSAやESIGNなどの公開鍵暗号技術を用いて実現可能であり、公開鍵暗号技術で必要となる秘密鍵と公開鍵のうち、電子署名生成者のみが知りうる秘密鍵を用いて署名対象である電子データを暗号化することにより、電子データに対する電子署名を生成することが可能となる。さらに、電子データ通信手段113は、コンピュータシステムが一般的に提供するファイル転送機能やファイル受信機能などを利用することにより容易に実現可能である。

## 2: 送信者Aに対する電子データ送信意志確認処理

中継サーバ40は、送信者Aが確かに電子データを受信者B端末20へ送付する意志があった事実を確認するため、電子データ通信手段411を用いて送信者A端末10から送付依頼申請書51を受理後、公開鍵証明証取得手段412を用いて送信者Aの公開鍵証明証を認証システム30から取得し、電子署名検証手段413を用いてこの公開鍵証明証内に含まれる公開鍵により送付依頼申請書51に付与された電子署名を検証して、送付依頼申請書51の送付者が確かに送信者Aであることを確認する。そして申請書51内に送付対象電子データとその送付先情報が含まれていることを確認した後、ここで確認した事実の証拠情報を保管するため、電子データ保管手段414を用いて送付依頼申請書51を2次記憶媒体へ保管する。

【0017】ここで、公開鍵証明証取得手段412は、公開鍵暗号技術で必要となる秘密鍵と公開鍵のうち、一般利用者に公開するための公開鍵を第三者機関である認証システム30へあらかじめ登録しておき、署名検証において署名検証対象者の公開鍵を必要とする場合に、認証システム30に対して利用者名等を検索キーとして公開鍵証明証の検索を依頼することにより、必要な公開鍵証明証の取得が実現可能であり、これらの処理は、認証システム30が一般に保持する公開鍵証明証配送機能や既存のディレクトリ参照技術などを用いて実現可能である。また、電子署名検証手段413は、電子署名生成手段112と対で利用される手段であり、既存の暗号技術を用いて実現可能である。この手段は、公開鍵証明証取得手段412を利用して取得した公開鍵証明証内に含まれる公開鍵と、検証対象である電子署名及び署名の生成対象である電子データを入力として、対象電子データに付与された電子署名が、確かに公開鍵証明証内に示された公開鍵の所有者により生成されたものであることの検証を可能とする。さらに、電子データ保管手段414は、コンピュータシステムが一般的に提供するファイル入出力機能などを利用することにより容易に実現可能である。

【0018】以上の処理と手段により、中継サーバ40において、送信者Aが確かに対象電子データを受信者B



端末 20 へ送付する意志があった事実を確認し、その証拠情報の保管が実現可能となる。

3: 受信者 B 端末への電子データ取得催促通知処理  
中継サーバ 40 は、送信者 A 端末 10 が指定した送付先の受信者 B 端末 20 に対して、中継サーバ 40 が受信者 B 端末 20 宛の電子データを保管していること及びこれを取得するための識別子よりなる電子データ取得催促通知 52 を、電子データ通信手段 411 を用いて通知する。

4: 電子データ取得催促通知受信処理  
受信者 B 端末 20 は、電子データ通信手段 213 を用いて 3 で送付された通知 52 を受理する。

5: 中継サーバへの電子データ取得申請処理  
受信者 B 端末 20 は、中継サーバ 40 に保管されている受信者 B 端末 20 宛の電子データを取得するため、電子データ編集手段 211 を用いて識別子に対応する電子データを取得するための電子データ取得申請書を作成し、電子署名生成手段 212 を用いて電子データ取得申請書に対する受信者 B の電子署名を生成し、電子データ通信手段 213 を用いて電子署名が付与された電子データ取得申請書 53 を中継サーバ 40 へ送付する。

6: 受信者 B に対する電子データ受信意志確認処理  
中継サーバ 40 は、受信者 B が確かに送信者 A 端末 10 から送付された電子データを受信する意志があった事実を確認するため、電子データ通信手段 411 を用いて受信者 B 端末 20 から電子データ取得申請書 53 を受理後、公開鍵証明証取得手段 412 を用いて受信者 B の公開鍵証明証を認証システム 30 から取得し、電子署名検証手段 413 を用いてこの公開鍵証明証内に含まれる公開鍵により電子データ取得申請書 53 に付与された電子署名を検証して、電子データ取得申請書 53 で指定された識別子に対応する電子データの送付先情報が、電子データ取得申請書 53 の送付者である受信者 B と一致していることを確認する。その後、ここで確認した事実の証拠情報を保管するため、電子データ保管手段 414 を用いて電子データ取得申請書 53 を 2 次記憶媒体へ保管する。

【0019】以上の処理と手段により、中継サーバ 40 において、送信者 A が送付した電子データを受信者 B が受理する意志があった事実を確認し、その証拠情報の保管が実現可能となる。

7: 受信者 B 端末への電子データ送付処理  
中継サーバ 40 は、電子データ通信手段 411 を用いて電子データ取得申請書 53 で指定された識別子に対応する電子データ 54 を受信者 B 端末 20 へ送付する。

8: 電子データ受信処理  
受信者 B 端末 20 は、電子データ通信手段 213 を用いて中継サーバ 40 が送付した電子データを受信する。

9: 受領証送付処理  
受信者 B 端末 20 は、電子データを受理したことを中継

サーバ 40 に対して通知するための受領証を送付するため、受領確認情報生成手段 217 を用いて受理した電子データを一意に特定可能な受領確認情報を生成し、データ編集手段 211 を用いて少なくとも受領確認情報と取得申請書で指定した識別子を含む受領証を生成する。そして、電子署名生成手段 212 を用いてこの受領証に対する受信者 B の電子署名を生成し、電子データ通信手段 213 を用いて電子署名が付与された受領証 55 を中継サーバ 40 へ送付する。

10 【0020】ここで受領確認情報生成手段 217 は、どの電子データを受理したのかを一意に特定する情報を生成するための手段であり、この手段は、例えばハッシュ化技術を用いて、受理した電子データに対するハッシュ値を生成し、これを受領確認情報とすることにより実現可能である。このことは、受理した電子データと、これを元に算出したハッシュ値が、確率統計上極めて 1 対 1 の関係を保持することが可能となるためである。またこのハッシュ化技術は、既存の MD5 や SHA-1 などが世の中で広く知られるところとなっている。

20 10: 受信者 B 端末への電子データ到達確認処理  
中継サーバ 40 において、受信者 B 端末 20 が確かに送信者 A 端末 10 が送付した電子データを受理した事実を確認するため、電子データ通信手段 411 を用いて受信者 B 端末 20 から受領証 55 を受理後、公開鍵証明証取得手段 412 を用いて受信者 B の公開鍵証明証を認証システムから取得し、電子署名検証手段 413 を用いてこの公開鍵証明証内に含まれる公開鍵により受領証 55 に付与された電子署名を検証して、受領証 55 の送付者が受信者 B 端末 20 であることを確認し、さらにこの受信者 B 端末 20 が、受領証 55 内に含まれる識別子に対応する電子データの送付先情報と一致していることを確認する。続いて、受信者 B 端末 20 が受理した電子データ 54 が、確かに送信者 A 端末 10 が送付依頼した電子データであることを確認するため、受領確認情報確認手段 415 を用いて受領証 55 内に含まれる受領確認情報が識別子に対応する電子データと同一の電子データを指し示すことを確認する。その後、ここで確認した事実の証拠情報を保管するため、電子データ保管手段 414 を用いて受領証 55 を 2 次記憶媒体へ保管する。

30 【0021】ここで、受領確認情報確認手段 415 は、受信者 B 端末 20 が受理した電子データが、送付した電子データと同一であることを確認するための手段であり、受領確認情報生成手段 217 で示したハッシュ化技術を用いて、電子データの送信者である中継サーバ 40 において、受信者 B 端末 20 へ送付した電子データに対するハッシュ値を生成し、これと受信者 B 端末 20 から受理した受領確認情報とを比較し、これらが一致することを確認することにより実現する。

50 【0022】以上の処理と手段により、中継サーバ 40 において、送信者 A 端末 10 が送付した電子データを受



信者B端末20が確かに受理した事実を確認し、その証拠情報の保管が実現可能となる。

11：受信者A端末への結果通知処理

中継サーバ40は、送信者A端末10に対して受信者B端末20への電子データ送付の結果を通知するため、電子データ通信手段411を用いて送付結果通知56を送信者A端末10へ送付する。

12：中継サーバからの結果通知確認処理

送信者A端末10は、電子データ通信手段113を用いて11で送付された結果通知56を受信し、電子データ表示手段117を用いて受信者B端末20へ電子データが到達したことを確認する。

【0023】ここで電子データ表示手段117は、コンピュータシステムが一般的に提供するエディタ機能などを利用することにより容易に実現可能である。以上の処理と手段により、送信者A端末10が送付した電子データを受信者B端末20が確かに受理した事実を、送信者Aが確認することが可能となる。

【0024】

【発明の効果】以上の説明から明らかであるように、この発明の方法とそれを実現する手段によって、送信者A

端末と受信者B端末の間で送受信された電子データに対して、送信者Aが電子データを受信者B端末に対して送付する意志があった事実及び、送信者A端末が送付した電子データを受信者Bが受理する意志があった事実及び、送信者A端末が送付した電子データを受信者B端末が確かに受理した事実を、後日、中継サーバが内部に保管している情報を提示することにより、外部の第三者に対して証明することが可能となる。また、中継サーバが送信者端末と受信者端末の間に介在して電子データの送受信の確認及び制御を行っているため、電子データの送受信を行う当事者の意志によらない確実な電子データの送達が可能となる。

【図面の簡単な説明】

【図1】この発明の装置構成を示すブロック図。

【図2】この発明における中継サーバを介した電子データ到達保証方法を実現するための処理の流れを示す図。

【図3】この発明を実現するための具体的実施例の処理の流れを、必要な手段とともに示す図。

【図4】Aは従来技術による電子データの到達確認方法のシステム構成を示す図、Bはその処理手順を示す図である。

【図1】

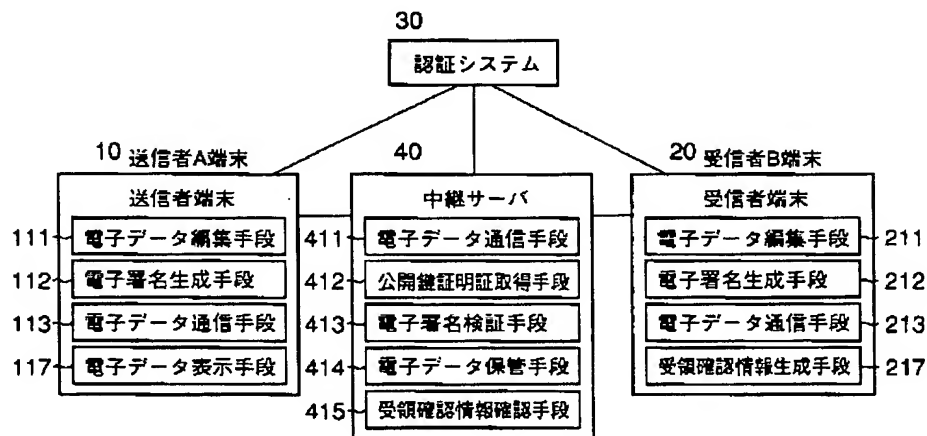


図 1 本発明における装置構成

【図 2】

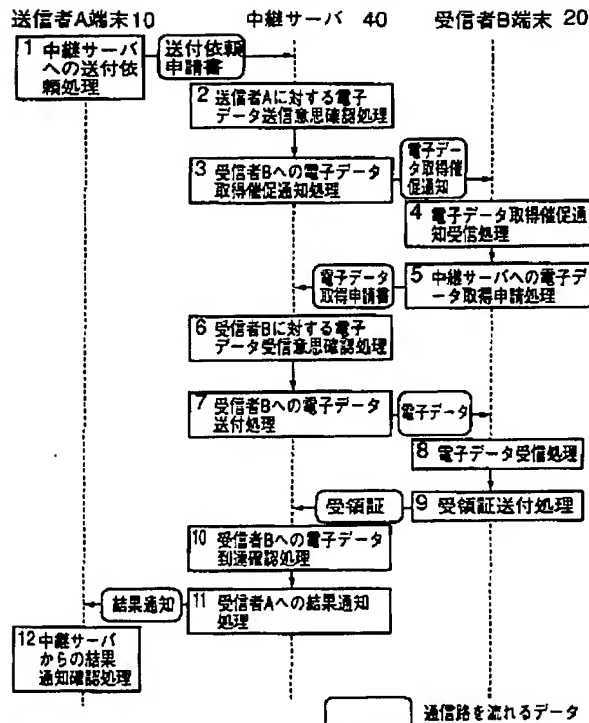


図 2 本発明における電子データ到達保証方法を実現するための処理の流れ

【図 3】

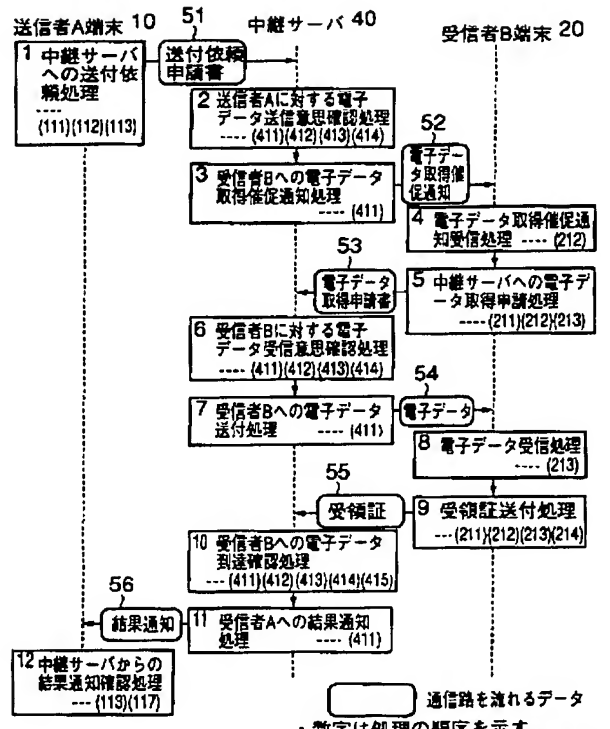


図 3 本発明を実現する具体的な実施例

【図 4】

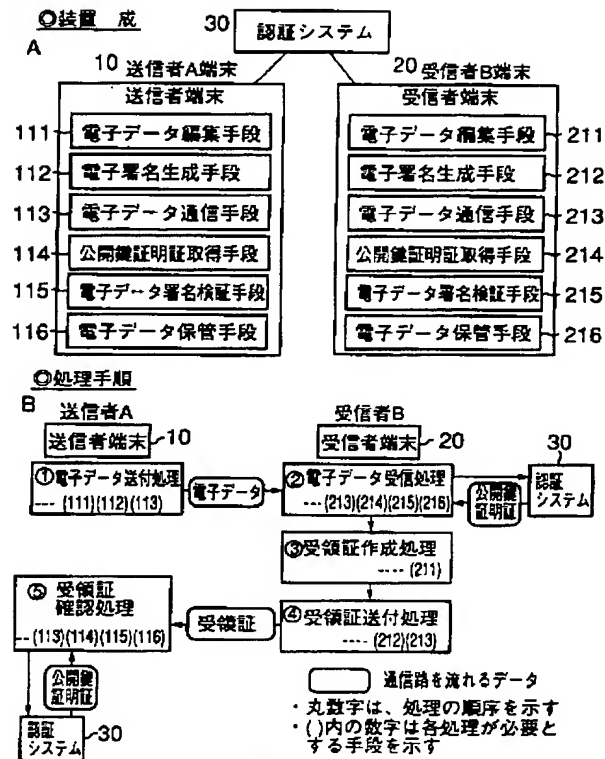


図 4 従来技術における電子データ到達確認方法

フロントページの続き

(51) Int. Cl. <sup>7</sup>

識別記号

F I

テーマコード\* (参考)

H 0 4 L 12/58